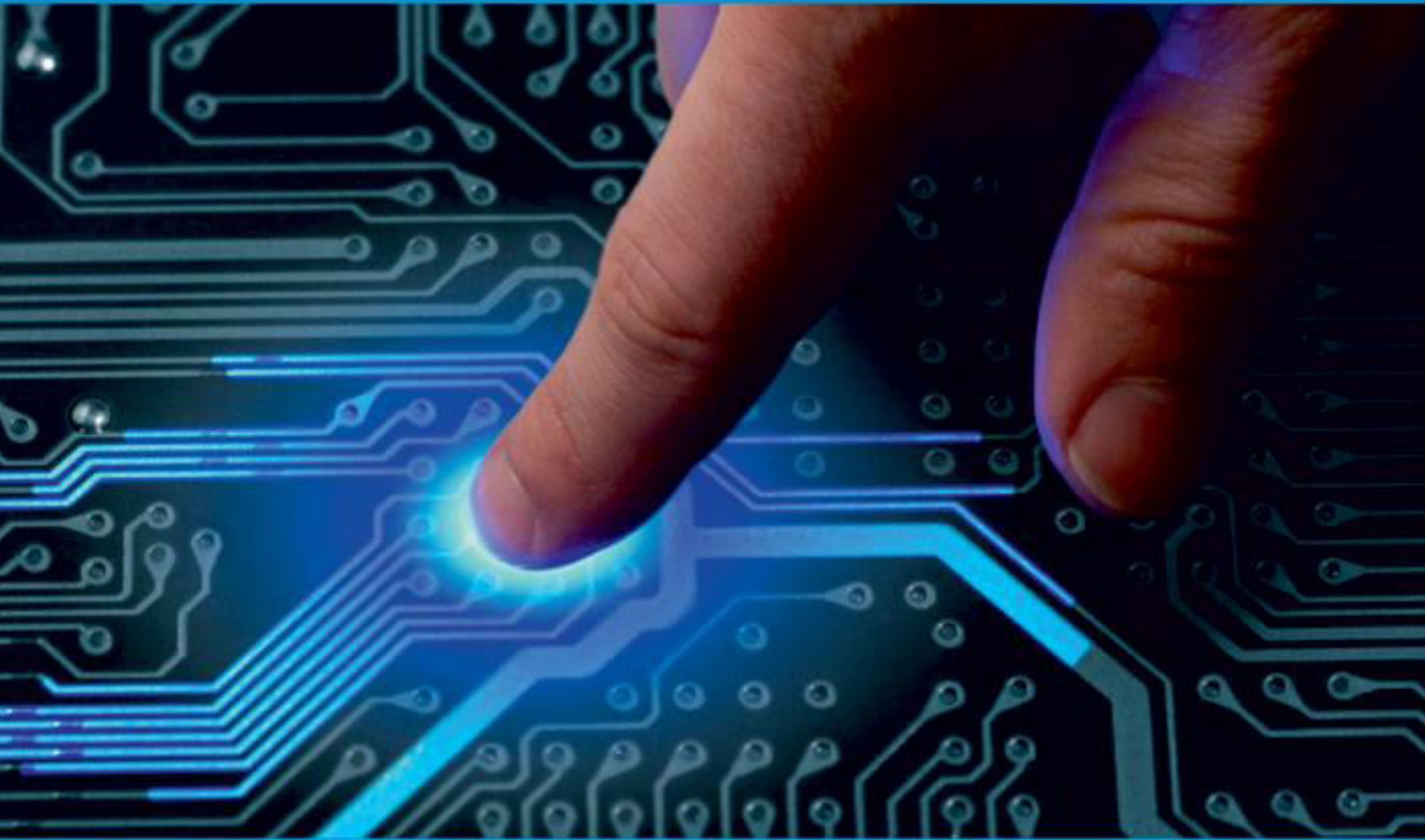
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 2, February 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1202061 |

Enhancing Intrusion Detection Systems through Distributed Ledger Technology for Secure Logging

Pradeep Bonumaddi, Murugan R

2nd year MCA (ISMS), School of Computer Science and IT, Jain (Deemed-to-be University)

Bangalore, India

Programme Head-MCA, School of Computer Science and IT, Jain (Deemed-to-be University)

Bangalore, India

ABSTRACT: Nodes in Mobile Ad Hoc Networks (MANETs) are limited battery powered. That's why energy efficient routing has become an important optimization criterion in MANETs. The conventional routing protocols do not consider energy of the nodes while selecting routes which leads to early exhaustion of nodes and partitioning of the network. This paper attempts to provide an energy aware routing algorithm. The proposed algorithm finds the transmission energy between the nodes relative to the distance and the performance of the algorithm is analyzed between two metrics Total Transmission energy of a route and Maximum Number of Hops. The proposed algorithm shows efficient energy utilization and increased network lifetime with total transmission energy metric.

KEYWORDS: DLT, blockchain, intrusion detection, secure logging, tamper resistance, smart contracts, privacy, compliance.

I. Introduction

The integration of Distributed Ledger Technology (DLT), often referred to as blockchain, with Intrusion Detection Systems (IDS) represents an innovative approach to enhance the security of logging mechanisms within a network. This fusion addresses several challenges associated with traditional centralized logging systems, providing a more secure and tamper-resistant solution.

Tamper-Resistant Logging: Traditional logging systems are vulnerable to attacks where unauthorized individuals may alter or delete log entries to cover their tracks. By leveraging DLT, a decentralized and immutable ledger is created, making it extremely difficult for attackers to manipulate or tamper with logged data. Each log entry is cryptographically linked to the previous one, forming a chain of blocks that ensures the integrity of the information.

Decentralization for Resilience: Centralized logging systems pose a single point of failure. If an attacker gains access to the centralized log server, they can compromise the entire log database. DLT introduces decentralization, where log entries are distributed across multiple nodes in the network. This makes it more challenging for attackers to disrupt or compromise the logging infrastructure, enhancing the overall resilience of the system.

Immutable Audit Trail: The transparent and immutable nature of DLT ensures that every action within the network is recorded and time-stamped. This creates a robust audit trail that can be invaluable for forensic analysis in the event of a security incident. Security professionals can trace the origin and progression of an attack more reliably, aiding in post-incident investigations.

Enhanced Trust and Accountability: The decentralized and transparent nature of DLT promotes trust within the network. Participants can verify the integrity of the logs independently, reducing the reliance on a central authority. This not only enhances accountability but also fosters a more trustworthy environment for network participants. Smart **Contracts for Automated Responses:** Smart contracts, programmable and self-executing scripts on the blockchain, can be utilized to automate responses based on predefined conditions. For example, if the IDS detects a specific type of intrusion, a smart contract could trigger predefined actions such as isolating the affected system or notifying security personnel.

Privacy and Compliance: DLT can also address privacy concerns by allowing for selective disclosure of information. Participants can have different levels of access to the logs based on their roles and responsibilities. Additionally, the transparency and traceability of DLT contribute to meeting compliance requirements in various industries.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1202061 |

Scalability: The distributed nature of DLT allows for scalability by enabling the addition of nodes to the network. This ensures that the logging infrastructure can accommodate the growing volume of data generated in larger networks without sacrificing performance.

II. Motivation

The motivation behind using Distributed Ledger Technology (DLT) for logging in intrusion detection stems from the need to address several critical challenges inherent in traditional logging systems. By leveraging the unique features of DLT, such as transparency, immutability, and tamper resistance, organizations can significantly enhance the security and reliability of their intrusion detection processes. Here are key motivations for adopting DLT in this context:

Transparency: DLT provides a transparent and decentralized ledger where every participant in the network has visibility into the log entries. This transparency ensures that all relevant stakeholders, including security professionals, can independently verify the integrity of the log data. It reduces the reliance on a central authority and fosters trust among network participants, as they can collectively monitor and validate the recorded activities.

Immutability: The immutability of DLT ensures that once a log entry is added to the blockchain, it cannot be altered or deleted retroactively. This property is crucial for maintaining the integrity of the log data. In the context of intrusion detection, having an immutable record of all activities and security events is essential for forensic analysis, post-incident investigations, and compliance with regulatory requirements.

Tamper Resistance: Traditional centralized logging systems are susceptible to tampering by malicious actors who seek to cover their tracks. DLT mitigates this risk by distributing log entries across multiple nodes in the network and linking them cryptographically in a chain of blocks. This makes it extremely difficult for an attacker to tamper with the logged information without being detected. The tamper-resistant nature of DLT adds an additional layer of security to the logging process.

Enhanced Forensic Analysis: The transparent and immutable nature of DLT facilitates more robust forensic analysis in the aftermath of a security incident. Security professionals can rely on the blockchain's history to reconstruct the sequence of events, identify the source of the intrusion, and understand the tactics employed by the attacker. This aids in developing effective response strategies and improving overall cybersecurity resilience.

Trust and Accountability: DLT promotes trust by providing a decentralized and verifiable record of activities. Participants can trust that the log data has not been manipulated, and accountability is enhanced as each participant can independently validate the information. This trust and accountability are crucial for collaborative security efforts, especially in multi-party or distributed environments.

Compliance with Regulations: Many industries and sectors are subject to regulatory requirements that mandate the secure and auditable handling of sensitive data, including security logs. DLT's features align well with these regulatory demands, offering a solution that not only meets compliance standards but also provides a more robust and transparent approach to log management.

III. Related work

The intersection of intrusion detection systems (IDS) and blockchain technology has emerged as a promising avenue in the realm of cybersecurity. In their comprehensive review, W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han delve into the synergistic integration of these two fields, shedding light on the potential benefits and challenges posed by their convergence. Published in IEEE Access in 2018, the paper explores the symbiotic relationship between intrusion detection mechanisms and blockchain, aiming to fortify the security landscape. By surveying existing literature and advancements in the field, the authors provide a nuanced understanding of how blockchain technology can enhance the robustness and transparency of intrusion detection systems. The review not only synthesizes key findings but also critically evaluates the implications and future directions of this interdisciplinary approach, offering valuable insights for researchers and practitioners navigating the evolving landscape of cybersecurity. The work contributes significantly to the discourse surrounding the fusion of intrusion detection and blockchain technologies, paving the way for further exploration and innovation in this dynamic field.

Al-E'mari et al highlights the vulnerabilities of traditional IDSs and how blockchain's distributed ledger, with its immutability and transparency, could be the key to overcoming them. The authors explore various proposed architectures, showcasing the potential for both signature-based and anomaly detection approaches. However, the path to widespread adoption isn't paved with roses. Scalability, performance overhead, and privacy concerns loom large, demanding further research and development. Standardization, regulatory frameworks, and seamless integration with existing security infrastructure are also crucial pieces of the puzzle. Although challenges remain, this paper provides compelling evidence that blockchain could be a game-changer for IDSs, offering a future where collaborative defense prevails against ever-evolving cyber threats.

Odeh and Abu Taleb (2023) propose an ensemble of deep learning models (CNNs, LSTMs, GRUs) to combat the evolving threat of cyberattacks in resource-constrained IoT devices. This combined approach outperforms individual models, achieving over 99.5% accuracy with minimal resource consumption. While promising, further optimization, real-world testing, and improved interpretability are necessary for practical deployment. This paper highlights the potential of ensemble learning for significantly enhancing IoT intrusion detection.

Abubakar et al. (2023) propose an efficient blockchain-based approach to enhance the accuracy of intrusion detection systems (IDS). Traditional IDSs struggle with data manipulation and lack of trust, hindering their effectiveness. The authors address this by leveraging blockchain's distributed ledger technology, offering immutability, transparency, and enhanced data integrity. Their proposed system focuses on distributed blockchain-based intrusion detection systems (DBIDS), enabling real-time network monitoring and faster intrusion detection compared to centralized systems. Additionally, the blockchain facilitates secure and tamper-proof storage of network logs, crucial for accurate threat analysis and response.

Although promising, the paper acknowledges limitations. Scalability and performance overhead require further optimization for large-scale deployments. Additionally, privacy concerns need to be addressed to ensure sensitive data protection.

Overall, Abubakar et al. demonstrate the potential of blockchain to significantly improve IDS accuracy and pave the way for future research towards addressing scalability, performance, and privacy challenges for wider adoption.

Khonde and Ulagamuthalvi (2022) propose a hybrid intrusion detection system (IDS) utilizing blockchain (BC-HyIDS) to overcome vulnerabilities and information sharing issues in traditional systems. Combining signature-based and anomaly-based detection, BC-HyIDS leverages blockchain for secure signature exchange within a distributed network. Results show improved accuracy, detection rate, and reduced false alarms compared to traditional solutions. However, scalability, integration with existing infrastructure, and standardized regulations require further exploration for real-world implementation. This paper signifies the potential of blockchain to enhance IDS capabilities, paving the way for future research to address these challenges.

The research aims to explore the integration of Distributed Ledger Technology (DLT) into Intrusion Detection Systems (IDS) for secure logging. The primary objectives of this research are as follows:

Evaluate the Feasibility of DLT Integration: Assess the technical feasibility of integrating DLT with existing Intrusion Detection Systems. Explore the compatibility, performance implications, and potential challenges associated with implementing DLT for secure logging in diverse network environments.

Enhance Transparency in Logging Mechanisms: Investigate how the use of DLT can enhance transparency in logging by providing a decentralized and auditable ledger. Examine the impact on the visibility of log entries for stakeholders, ensuring that all relevant parties can independently verify the recorded activities.

Achieve Immutable and Tamper-Resistant Logging: Implement and analyze the tamper-resistant nature of DLT to ensure that log entries are immutable once added to the blockchain. Evaluate the effectiveness of DLT in preventing unauthorized alterations or deletions of logged data, thus maintaining the integrity of the intrusion detection logs.

Improve Forensic Analysis Capabilities: Explore how the integration of DLT with IDS can enhance forensic analysis capabilities. Investigate the blockchain's role in reconstructing the sequence of security events, identifying the source and tactics of intrusion, and facilitating more effective post-incident investigations.

Assess Trust and Accountability in Network Security: Evaluate the impact of DLT on establishing trust and accountability within a network. Analyze how the decentralized and transparent nature of DLT contributes to building trust among network participants and enhances accountability for security-related activities.

Automate Responses Through Smart Contracts: Explore the use of smart contracts within DLT for automating responses to security events detected by the IDS. Investigate how programmable and self-executing scripts can be leveraged to trigger predefined actions in real-time, improving the speed and efficiency of incident response.

Address Privacy Concerns and Compliance Requirements: Investigate how DLT can address privacy concerns in logging mechanisms by allowing for selective disclosure of information based on participants' roles. Assess the compliance implications of integrating DLT with IDS, ensuring that the solution aligns with regulatory requirements and industry standards.

Evaluate Scalability and Performance: Assess the scalability of the DLT-based logging system to accommodate the growing volume of data generated in larger networks. Evaluate the performance implications and identify potential scalability challenges to ensure the practicality of the proposed solution in diverse network environments.

Expected Outcomes:

A comprehensive understanding of the technical feasibility and challenges associated with integrating DLT into IDS for secure logging. Improved transparency and tamper resistance in logging mechanisms, enhancing the reliability of intrusion detection logs. Enhanced forensic analysis capabilities, providing a more reliable and detailed reconstruction of security events. Increased trust and accountability within network security, fostering a more secure and collaborative environment. Smart contract-based automation for incident response, improving the efficiency of security operations. A solution that addresses privacy concerns and complies with relevant regulations and standards. Insights into the scalability and performance of DLT-based logging systems in different network environments.

IV. METHODOLOGY

1.System Architecture: The conceptual system architecture integrates Distributed Ledger Technology (DLT) into an Intrusion Detection System (IDS) for secure logging. The architecture consists of the following key components: **Intrusion Detection System (IDS):** Monitors network activities and detects potential security incidents.
Blockchain Network: Utilizes a decentralized and distributed ledger for secure logging.
Smart Contracts: Programmable scripts that automate predefined responses to security events.
Nodes: Participants in the blockchain network responsible for validating and adding log entries.
Description: The IDS generates security events and sends them to the blockchain network. Smart contracts may be triggered based on predefined conditions, automating responses. Nodes reach consensus on the validity of log entries, ensuring tamper resistance. The blockchain ledger stores immutable and transparent log data.
2.Data Structure: The data structure for logging on the blockchain includes the following components:
Transaction Data:
Event Type: Describes the nature of the security event (e.g., intrusion attempt, malware detection).
Source and Destination Addresses: Identify the network entities involved.
Timestamp: Records the time when the security event occurred.
Event Details: Specific information about the security incident.
Metadata:
Hash Value: Cryptographic hash to ensure integrity.
Digital Signatures: Used for authentication and to verify the origin of log entries.
Smart Contracts:
Conditions: Predefined criteria triggering automated responses.
Actions: Specified actions to be executed upon triggering.
3.Consensus Mechanism: The choice of consensus mechanism is crucial for maintaining the integrity and security of the logging system. Different consensus mechanisms can be explored:
Proof of Work (PoW): Nodes must solve complex mathematical problems to add a block, requiring computational power. Provides high security but may have scalability challenges.
Proof of Stake (PoS): Nodes are chosen to create a new block based on the amount of cryptocurrency they hold or stake. It is energy-efficient compared to PoW but requires trust in wealth distribution.
Practical Byzantine Fault Tolerance (PBFT): A consensus algorithm suitable for permissioned blockchains where a predetermined set of nodes reaches consensus. Offers high throughput but requires a trust assumption on the reliability of nodes.
The choice of consensus mechanism depends on factors like the network's characteristics, desired level of decentralization, and the balance between security and scalability. This system architecture, data structure, and consensus mechanism provide a foundation for the integration of DLT into an IDS for secure logging, ensuring transparency, immutability, and a tamper resistant environment for critical security data.

V. CONCLUSION AND FUTURE WORK

The integration of Distributed Ledger Technology (DLT) into Intrusion Detection Systems (IDS) for secure logging presents a promising avenue for enhancing cybersecurity. Leveraging blockchain's transparency, tamper resistance, and smart contracts, our proposed system establishes a foundation for robust and automated incident response. The architecture addresses privacy concerns and compliance requirements, fostering trust and accountability within network security.

Need for Future Work:

While the methodology outlined in this research lays the groundwork for a secure logging system, future work should focus on several areas. Firstly, further exploration is required to assess the scalability of the DLT-based logging system in large and dynamic network environments. Additionally, ongoing research should delve into refining smart contracts for more complex and adaptive incident response strategies. Moreover, continuous efforts are needed to stay abreast of evolving cybersecurity threats, ensuring that the proposed framework remains resilient and adaptive in the face of emerging challenges. Finally, real-world implementation and testing are essential to validate the practical viability of the proposed system and its effectiveness in diverse network scenarios.

REFERENCES

1. Meng, W., Tischhauser, E. W., Wang, Q., Wang, Y., & Han, J. (2018). When Intrusion Detection Meets Blockchain Technology: A Review. IEEE Access, 6, 10179-10188.
2. Al-E'mari, S., Anbar, M., Sanjalawe, Y., Manickam, S., & Hasbullah, I. (2022). Intrusion Detection Systems Using Blockchain Technology: A Review, Issues and Challenges. Computer Systems Science & Engineering, 40(1), 87–112.
3. Odeh, A., & Abu Taleb, A. (2023). Ensemble-Based Deep Learning Models for Enhancing IoT Intrusion Detection. Applied Sciences (2076-3417), 13(21), 11985.
4. Abubakar, A. A., Liu, J., & Gilliard, E. (2023). An efficient blockchain-based approach to improve the accuracy of intrusion detection systems. Electronics Letters (Wiley-Blackwell), 59(18), 1–3.
5. S. R. Khonde, & V. Ulagamuthalvi. (2022). Hybrid intrusion detection system using blockchain framework. EURASIP Journal on Wireless Communications and Networking, 2022(1), 1–25.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING